(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 31 395 A 1**

(51) Int. Cl.[7]:
G 08 C 17/02
G 05 B 19/04
B 60 R 11/02
B 60 R 16/02
B 60 R 25/00

(21) Aktenzeichen: 101 31 395.0
(22) Anmeldetag: 28. 6. 2001
(43) Offenlegungstag: 23. 1. 2003

(71) Anmelder:
DaimlerChrysler AG, 70567 Stuttgart, DE

(72) Erfinder:
Dürschmidt, Ferry, Dipl.-Phys., 71292 Friolzheim, DE; Krauth, Andrej, Dip.-Ing., 73728 Esslingen, DE; Müller, Michael, Dipl.-Ing.(BA), 70374 Stuttgart, DE

(56) Entgegenhaltungen:
DE 197 50 372 A1
DE 42 18 804 A1
DE 689 20 462 T2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Übertragen von Software- Modulen

(57) Die Erfindung betrifft eine Verfahren zum Übertragen von Software-Modulen von einer Zentrale zu einer mobilen Vorrichtung, insbesondere zu einem Verkehrs- oder Transportmittel. Für die Übertragung wird eine Einrichtung zur drahtlosen Datenübertragung in beiden Richtungen verwendet, und eine Menge von Software-Modulen wird ausgewählt. Die aktuelle Konfiguration der mobilen Vorrichtung wird an die Zentrale übermittelt. Geprüft wird, welche dieser Software-Module für die aktuelle Konfiguration freigegeben sind. Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden übertragen. Vorzugsweise werden für die Ziel-Geräte Geräte-Typ-Kennungen und für die Software-Module Software-Typ-Kennungen in Freigabe-Festlegungen verwendet. Diese Freigabe-Festlegungen werden bei einer Freigabe-Prüfung verwendet. Das Verfahren ist in gleicher Weise für die Versorgung einer einzelnen mobilen Vorrichtung wie auch für Familien von variantenreichen oder variantenarmen mobilen Vorrichtungen anwendbar.

DE 101 31 395 A 1

DE 101 31 395 A 1

BNSDOCID: <DE_____10131395A1_I_>

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Übertragen von Software-Modulen von einer Zentrale zu einer mobilen Vorrichtung, vorzugsweise zu einem Verkehrs- oder Transportmittel, mit Hilfe einer Einrichtung zur drahtlosen Datenübertragung in beide Richtungen.

[0002] In mobilen Vorrichtungen, insbesondere in Kraftfahrzeugen, wird eine steigende Anzahl von Geräten verwendet, die durch Software-Module gesteuert werden, z. B. Tür-Steuergeräte. Manche Geräte, z. B. elektronische Navigationssysteme und Systeme zur Sprachausgabe, benötigen umfangreiche Datenbibliotheken. Um mobile Vorrichtungen an individuelle Anforderungen und Wünsche von Benutzern oder Betreibern anzupassen, werden oft Ziel-Geräte in vielen unterschiedlichen Versionen und Varianten hergestellt und eingebaut, manchmal auch nachträglich. Durch die Kombination von Varianten entsteht eine hohe Zahl unterschiedlicher Konfigurationen von Ziel-Geräten an Bord von mobilen Vorrichtungen, die zu einer Familie von mobilen Vorrichtungen gehören. Der Hersteller einer mobilen Vorrichtung hat trotz der Variantenvielfalt zu gewährleisten, daß diese Ziel-Geräte in jeder freigegebenen Kombination im laufenden Betrieb sicher zusammenspielen.

[0003] Mit "Software-Module" werden insbesondere Programme oder Teile von Programmen, die an Bord von mobilen Vorrichtungen ausgeführt werden, und Daten für solche Programme oder für Ziel-Geräte sowie Parameter von Ziel-Geräten bezeichnet. Mit "Ziel-Geräten" werden diejenigen datenverarbeitenden Geräte an Bord einer mobilen Vorrichtung bezeichnet, für die Software-Module zu übertragen sind, hierzu zählen insbesondere Steuergeräte z. B. für Türen oder die Klimaanlage. Ein zu übertragender Parameter beeinflußt beispielsweise die Funktionsweise eines Ziel-Geräts oder aktiviert oder deaktiviert ein Programm an Bord der mobilen Vorrichtung.

[0004] Es ist heute noch üblich, zum nachträglichen Übertragen von Software-Modulen in mobile Vorrichtungen die Ziel-Geräte z. B. in einer Werkstatt auszubauen, mit den gewünschten Software-Modulen zu versehen und dann wieder einzubauen. In manchen Fällen muß das Ziel-Gerät sogar zum Hersteller geschickt werden, der zentral die Software-Module überträgt. Diese Wege sind teuer und zeitaufwendig.

[0005] Aus DE 197 50 372 A1 ist ein Verfahren zum Übertragen von Programmen und/oder Daten von einem zentralen Server an ein Fahrzeug bekannt. Die Übertragung erfolgt per Funkverbindung. Fahrzeug und Server haben je ein Sende- und Empfangsgerät. Die Zugriffsberechtigung des Benutzers wird geprüft, hierzu werden Daten vom Fahrzeug an die Zentrale gemeldet.

[0006] In DE 198 53 000 A1 wird ein Verfahren zum Versorgen von Kraftfahrzeugen mit Daten sowie zum Austausch, Abfragen, Ändern, Aktualisieren von Daten offenbart. Verwendet wird eine drahtlose Datenübertragungseinrichtung. Die Daten sind vorzugsweise Überwachungsdaten, z. B. Betriebsdaten von Bremsen, Fahrwerk, Ölstand, oder Programme oder Programmteile.

[0007] Aus DE 195 32 067 C1 ist ein Verfahren zum Einprogrammieren von Daten in ein Fahrzeug-Bauteil bekannt. Daten werden von einer Zentrale an die anfordernde Stelle übertragen. Insbesondere um unberechtigten Zugriff auf die übertragenen Daten zuverlässig zu unterbinden, werden Informationen zur Identität von Fahrzeug, Bauteil und Nutzer an die Zentrale übermittelt.

[0008] Aus DE 199 21 845 A1 ist eine Diagnosetestvorrichtung für Kraftfahrzeuge mit programmierbaren Steuergeräten bekannt. Ein externer Diagnosetester ist mit einer Programmerkennungs- und Programmladevorrichtung ausgestattet. Bei Bedarf wird die jeweils aktuellste Version eines Programms in den Programmspeicher des entsprechenden Steuergeräts geladen.

[0009] Die oben genannten Druckschriften offenbaren Verfahren, um Software-Module an eine mobile Vorrichtung zu übermitteln und dabei bei Bedarf Berechtigungs- und Freigabeprüfungen durchzuführen. Die Prüfungen beziehen sich jeweils auf eine einzelne mobile Vorrichtung. Jedoch wird bei den Verfahren nicht die Möglichkeit berücksichtigt, daß Software-Module an variantenreiche mobile Vorrichtungen zu übertragen sind. Der Variantenreichtum wird auch nicht dadurch berücksichtigt, daß – wie in DE 198 53 000 A1 – Überwachungsdaten vom Fahrzeug an die Zentrale übermittelt werden. Der Variantenreichtum resultiert beispielsweise daher, daß in verschiedenen Exemplaren einer Familie von mobilen Vorrichtungen, z. B. einer Fahrzeugflotte, unterschiedliche Ziel-Geräte eingebaut sind oder daß Ziel-Geräte in unterschiedlichen Versionen und Varianten verwendet werden oder verschiedene Software-Module aktiviert worden sind. Der Variantenreichtum kann zu einer riesigen Zahl unterschiedlicher Prüfungen führen, die nicht mit vertretbarem Aufwand definiert und validiert werden können. Weiterhin wird nicht die Möglichkeit berücksichtigt, daß ein Benutzer oder Betreiber einer mobilen Vorrichtung ein Ziel-Gerät erneuert oder nachträglich ergänzt, ohne daß der Hersteller der mobilen Vorrichtung hierüber informiert wird und dies bei einer Freigabe-Prüfung nach dem Stand der Technik berücksichtigen kann. Auch beim Verfahren nach DE 195 32 067 C1, bei dem Informationen über die Fahrzeug-Identität an die Zentrale übermittelt werden, werden nachträgliche Änderungen nicht berücksichtigt. Zwar kann die Zentrale sich eine abgespeicherte Konfigurations-Datei des Fahrzeugs beschaffen, diese Informationen können aber falsch oder veraltet sein.

[0010] Variantenreichtum und nachträgliche Änderungen sind aber zu berücksichtigen, um sicherzustellen, daß zu jeder mobilen Vorrichtung die richtigen Software-Module übertragen werden und sichergestellt wird, daß die übertragenen Software-Module auf dem Fahrzeug fehlerfrei miteinander und mit den Ziel-Geräten an Bord zusammenspielen und nicht zu unerwünschten oder fehlerhaften Betriebszuständen führen.

[0011] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren der eingangs beschriebenen Art zu schaffen, das die beschriebenen Nachteile vermeidet. Insbesondere soll gewährleistet werden, daß bei variantenreichen Familien von mobilen Vorrichtungen mit Ziel-Geräten verschiedener Hersteller oder bei nachträglichen Änderungen an einzelnen mobilen Vorrichtungen nur die richtigen und keine anderen Software-Module übertragen werden. Weiterhin ist eine Vorrichtung zur Durchführung des Verfahrens zu schaffen.

[0012] Die Aufgabe wird durch ein Verfahren nach Anspruch 1 und durch eine Vorrichtung nach Anspruch 12 gelöst. Vorteilhafte Ausgestaltungen werden durch die Unteransprüche beschrieben.

[0013] Für die Übertragung wird eine Einrichtung zur drahtlosen Datenübertragung in beiden Richtungen verwendet,

und eine Menge von Software-Modulen wird ausgewählt. Diese Menge besteht aus mehreren Software-Modulen oder aus nur einem einzigen Software-Modul. Informationen über die aktuelle Konfiguration der mobilen Vorrichtung werden an die Zentrale übermittelt. Diese Informationen umfassen eine Auflistung, welche Ziel-Geräte und welche Software-Module vor Beginn der Übertragung an Bord der mobilen Vorrichtung tatsächlich vorhanden sind. Geprüft wird, welche dieser Software-Module für die aktuelle Konfiguration freigegeben sind. Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden übertragen.

[0014] Vorzugsweise werden für eine Freigabe-Prüfung Freigabe-Festlegungen verwendet, die wie folgt erzeugt werden (Anspruch 2): Für die Ziel-Geräte werden Geräte-Typ-Kennungen festgelegt, also Kennungen für die Typen von Ziel-Geräten. Für die Software-Module werden Software-Typ-Kennungen festgelegt. Unter Verwendung der Geräte-Typ-Kennungen und Software-Typ-Kennungen wird festgelegt, welche der ausgewählten Software-Module für welche Typen von Ziel-Geräten freigegeben sind.

[0015] Diese Freigabe-Festlegungen werden bei der Freigabe-Prüfung verwendet.

[0016] Das Verfahren ist in gleicher Weise für die Versorgung einer einzelnen mobilen Vorrichtung wie auch für Familien von variantenreichen oder variantenarmen mobilen Vorrichtungen anwendbar. Insbesondere werden auch dann zuverlässig die richtigen und keine anderen Software-Module ausgewählt und übertragen, wenn in der mobilen Vorrichtung mehrere Ziel-Geräte unterschiedlicher Hersteller vorhanden sind und diese Ziel-Geräte in unterschiedlichen Versionen und Varianten vorkommen, die unterschiedliche Software-Module benötigen.

[0017] Die richtigen Software-Module werden auch dann ausgewählt und übertragen, wenn ein Benutzer oder Betreiber der mobilen Vorrichtung ein Ziel-Gerät durch ein andersartiges ersetzt hat oder nachträglich ein weiteres Ziel-Gerät ergänzt hat. Dies wird insbesondere dadurch erreicht, daß ermittelt wird, welche Ziel-Geräte und Software-Module sich zum Zeitpunkt der Übertragung tatsächlich in der mobilen Vorrichtung befinden. Nicht mehr erforderlich ist es, eine Abfrage in einer zentralen Datenbank mit Konfigurationen von mobilen Vorrichtungen durchzuführen. Die Einträge in einer solchen zentralen Datenbank können veraltet sein, z. B. weil ein Ziel-Gerät durch ein andersartiges ersetzt wurde oder ein Ziel-Gerät ergänzt oder entfernt wurde, ohne daß der Hersteller hierüber informiert wurde.

[0018] Dank der Verwendung einer drahtlosen Datenübertragungseinrichtung ist es nicht erforderlich, daß die mobile Vorrichtung zum Übertragen in eine Werkstätte gefahren oder transportiert wird. Es ist möglich, ein Software-Modul bereits unmittelbar nach seiner Fertigstellung und/oder Freigabe zu übertragen.

[0019] Einige beispielhafte Anwendungen, in denen das erfindungsgemäße Verfahren Vorteile gegenüber dem Stand der Technik erbringt, sind die folgenden:

- Auf Initiative des Kundendienstes eines Fahrzeugherstellers wird eine Kundendienstmaßnahme für alle Fahrzeuge eines Typs durchgeführt. Beispielsweise wird für alle Fahrzeuge einer Baureihe und eines Baujahrs eine neue Version eines Software-Moduls übertragen. Oder eine gesetzliche Bestimmung in einem Staat wird geändert, und Software-Module werden an Fahrzeuge in diesem Staat übertragen, um den geänderten Gesetzen nachzukommen. Besitzer und Nutzer der mobilen Vorrichtung werden informiert, und die Software-Module werden bei Einverständnis erfindungsgemäß übertragen. Durch das erfindungsgemäße Verfahren ist es nicht erforderlich, daß ein Fahrzeug des Typs in eine Werkstatt gebracht wird, und es wird sichergestellt, daß die neue Version des Software-Moduls nur auf diejenigen Fahrzeuge übertagen wird, für deren Konfigurationen sie freigegeben ist.
- Für einen bestimmten Fahrzeugtyp sollen umfangreiche Betriebsdaten an Bord aufgezeichnet, vorverarbeitet und an eine Zentrale übermittelt werden. Ein Programm, das die Aufzeichnung, Vorverarbeitung und Übermittlung übernimmt und dabei die Daten gegen unbefugten Zugriff sichert, wird durch das erfindungsgemäße Verfahren übertragen, nachdem der Eigentümer hierzu sein Einverständnis gegeben hat. Durch die Kenntnis der aktuellen Konfiguration wird sichergestellt, daß das übertragene Programm auf die tatsächlich an Bord vorhandenen Geräte zugeschnitten ist.
- Ein Besitzer einer mobilen Vorrichtung kauft vom Hersteller der mobilen Vorrichtung eine zusätzliche oder verbesserte Funktionalität, die ausschließlich durch zusätzliche Software-Module auf bereits eingebauten Ziel-Geräten realisiert wird. Durch das Verfahren wird es ermöglicht, daß die Software-Module ohne einen Werkstattbesuch übertragen werden, wenn eine drahtlose Verbindung hergestellt werden kann. Sichergestellt wird, daß die Software-Module für die mobile Vorrichtung freigegeben sind.
- Ein Ziel-Gerät an Bord eines Fahrzeugs ist ausgefallen, und das Fahrzeug kann seine Fahrt nicht fortsetzen. Ein Wartungstechniker fährt mit einem neuen Ziel-Gerät zum Fahrzeug. Das neue Gerät ist hinsichtlich der Hardware baugleich oder wenigstens funktionsgleich zum ausgefallenen Gerät, jedoch sind keine Software-Module in ihm abgespeichert. Die benötigten Software-Module werden durch das erfindungsgemäße Verfahren übertragen. Dadurch ist es nicht erforderlich, daß der Wartungstechniker die Software-Module sowie eine Einrichtung zur Konfigurations-Ermittlung und Freigabe-Prüfung mit sich führt. Da der Wartungstechniker für eine Flotte von unterschiedlichen Fahrzeugen mit verschiedenen Geräten an Bord verantwortlich ist, ist es wegen der Variantenvielfalt nicht möglich, daß er alle Software-Module mit sich führt, die beim Ausfall eines Ziel-Geräts an Bord eines der Fahrzeuge benötigt werden. Das erfindungsgemäße Verfahren spart erheblich Zeit gegenüber dem Vorgehen ein, daß der Wartungstechniker erst nach einem Ausfall eines Geräts ermittelt, welche Software-Module für das neue Gerät benötigt werden, und diese Software-Module dann von einer Zentrale beschafft.

[0020] Dank der Ausgestaltung nach Anspruch 3 kann das erfindungsgemäße Verfahren auch dann durchgeführt werden, wenn die aktuelle Konfiguration nicht komplett an die Zentrale übermittelt werden kann und daher benötigte Informationen fehlen, beispielsweise weil nicht alle Informationen über die aktuelle Konfiguration an Bord abgespeichert worden sind oder weil die Datenverbindung von der mobilen Vorrichtung zur Zentrale gestört ist. Hingegen haben diejenigen Informationen über die aktuelle Konfiguration, die an die Zentrale übermittelt wurden und nicht unzutreffend sind, Vorrang vor den abgespeicherten Konfigurations-Informationen.

[0021] Gemäß der Ausgestaltung nach Anspruch 3 werden Informationen über eine der Zentrale bekannten Konfigu-

ration der mobilen Vorrichtung in einem Konfigurations-Management-System oder Dokumentations-System abgespeichert. Beispielsweise umfaßt das System eine Datenbank, in der ein Datensatz für die mobile Vorrichtung bei ihrer Fertigstellung angelegt wird. Während der Übertragung wird eine Kennung der mobilen Vorrichtung zur Zentrale übermittelt. Diese Kennung unterscheidet diese mobile Vorrichtung wenigstens von allen anderen mobilen Vorrichtungen desselben Herstellers. Die an die Zentrale übermittelten Informationen über die aktuelle Konfiguration werden mit den abgespeicherten Informationen über die Konfiguration verglichen. Nachdem die Kennung der mobilen Vorrichtung an die Zentrale übermittelt wurde, wird auf den Datensatz für diese mobile Vorrichtung zugegriffen. Nicht übermittelte Informationen über die aktuelle Konfiguration werden durch Lesezugriff auf die abgespeicherte Konfiguration ergänzt. Auf die abgespeicherte Konfiguration wird insbesondere dann zugegriffen, wenn die aktuelle Konfiguration nur unvollständig an die Zentrale übermittelt wird und daher benötigte Informationen über die aktuelle Konfiguration, beispielsweise der Typ eines tatsächlich zum Zeitpunkt der Übertragung eingebauten Tür-Steuergerätes, fehlen. Bevorzugt werden die an die Zentrale übermittelten Informationen über die aktuelle Konfiguration einer Plausibilitätsprüfung unterzogen, um insbesondere Übertragungsfehler zu erkennen. Werden hierbei einzelne Informationen als offensichtlich unzutreffend erkannt, so werden die unzutreffenden der übermittelten Informationen durch die entsprechenden abgespeicherten Informationen ersetzt.

[0022] Anspruch 4 sieht vor, daß vor der Übertragung der Software-Module geprüft wird, ob mit Hilfe der drahtlosen Datenübertragungseinrichtung ein Übertragungskanal mit einer für die Übertragung ausreichenden Güte aufgebaut werden kann. Insbesondere wird geprüft, ob überhaupt eine Verbindung aufgebaut wird und ob diese Verbindung eine ausreichende Bandbreite besitzt. Bevorzugt werden die Software-Module vor der Übertragung komprimiert und nach der Übertragung dekomprimiert, um Übertragungszeit einzusparen.

[0023] Die Übertragung kann sowohl von der Zentrale als auch von einer Stelle außerhalb der Zentrale, beispielsweise einem Eigentümer, Fahrer oder Nutzer der mobilen Vorrichtung, angefordert werden, beispielsweise mit Hilfe eines Rechners im Internet. Die Stelle kann auch die mobile Vorrichtung oder ein Ziel-Gerät sein, das automatisch die Übertragung anfordert. Bevorzugt wird vor der Übertragung eine Berechtigungsprüfung für die anfordernde Stelle durchgeführt (Anspruch 5). Hierfür werden Informationen über die Identität der Stelle, welche die Übertragung der Software-Module anfordert, an die Zentrale übermittelt. Beispielsweise werden von einer anfordernden Person eine PIN, ein Paßwort oder ein Fingerabdruck ermittelt und mit abgespeicherten Informationen verglichen. Nur bei erfolgreicher Berechtigungsprüfung werden Software-Module übertragen. Durch die Berechtigungsprüfung wird insbesondere vermieden, daß ein Nutzer sich in den Besitz eines kostenpflichtigen Software-Moduls bringt, ohne dafür bezahlt zu haben, und daß die Übertragung aufgrund eines Fehlers ausgelöst wird.

[0024] Um zu verhindern, daß ein Software-Modul beispielsweise bei der Abspeicherung auf der mobilen Speicher-Einrichtung oder der Übertragung verfälscht oder manipuliert oder eine unberechtigt angefertigte Kopie verwendet wurde, wird eine Korrektheitsprüfung durchgeführt (Anspruch 6). Hierzu wird für mindestens ein Software-Modul eine Signatur erzeugt und auf der mobilen Speicher-Einrichtung abgespeichert. Die Signatur wird vorzugsweise dadurch erzeugt, daß das Software-Modul als Datenstrom behandelt wird und ein Hash-Wert erzeugt wird. Mit Hilfe eines geheimen Schlüssels wird aus diesem Hash-Wert die Signatur erzeugt. Die Signatur hängt also vom Software-Modul und vom geheimen Schlüssel ab.

[0025] Weiterhin wird an Bord der mobilen Vorrichtung für mindestens einen Ziel-Geräte-Typ ein öffentlicher Schlüssel abgespeichert. Mit Hilfe dieses öffentlichen Schlüssels wird die Signatur geprüft. Nur bei positivem Ausgang der Prüfung wird das Software-Modul als nicht verfälscht und als berechtigt erkannt.

[0026] Die Menge von Software-Modulen wird beispielsweise wie folgt ausgewählt (Anspruch 7): Die an die Zentrale übermittelte aktuelle Konfiguration der mobilen Vorrichtung wird mit einer Wunsch- oder Soll-Konfiguration verglichen. Eine Wunsch-Konfiguration wird beispielsweise dadurch erzeugt, daß ein Eigentümer der mobilen Vorrichtung zusätzliche Funktionalitäten erwirbt, eine Soll-Konfiguration dadurch, daß der Hersteller der mobilen Vorrichtung vorsieht, daß alle mobilen Vorrichtungen einer Baureihe mit einem bestimmten Software-Modul versorgt werden. Die Software-Module werden in Abhängigkeit von der Abweichung zwischen aktueller und Wunsch- bzw. Soll-Konfiguration ausgewählt. Beispielsweise werden alle Software-Module ausgewählt, die in der Wunsch- bzw. Soll-Konfiguration auftreten, aber in der aktuellen Konfiguration gar nicht oder nur in einer älteren Version.

[0027] Bevorzugt werden die Software-Module nach der Übertragung zunächst in einem Pufferspeicher an Bord der mobilen Vorrichtung abgespeichert. Sie werden dann an die jeweiligen Ziel-Geräte verteilt und zu diesen übertragen. Gemäß Anspruch 8 werden daher gemeinsam mit den Software-Modulen Meta-Informationen übertragen, die die Verteilung und/oder Übertragung und/oder Aktivierung der Software-Module an Bord der mobilen Vorrichtung steuern.

[0028] Die übertragenen Software-Module werden bevorzugt nur dann aktiviert, wenn die mobile Vorrichtung sich in einem sicheren Zustand befindet. Ansonsten besteht die Gefahr, daß während der Aktivierung eines Software-Moduls oder der dafür erforderlichen Deaktivierung eines zuvor vorhandenen Software-Moduls die mobile Vorrichtung in einen unerwünschten Betriebszustand gerät. Beispielsweise ist sicherzustellen, daß Software-Module für Steuergeräte an Bord eines Kraftfahrzeuges nur bei stehendem Fahrzeug aktiviert werden. Anspruch 9 sieht vor, daß zusätzlich Informationen über den aktuellen Betriebszustand der mobilen Vorrichtung an die Zentrale übermittelt werden. In Abhängigkeit von den Betriebszustands-Informationen wird entschieden, ob die mobile Vorrichtung sich in einem sicheren Zustand befindet. Dann, wenn sie sich in einem sicheren Zustand befindet, werden die übertragenen Software-Module aktiviert.

[0029] Die drahtlose Datenverbindung zwischen Zentrale und mobiler Vorrichtung kann gestört sein, weswegen die Übertragung der Software-Module nicht fehlerfrei abgeschlossen werden kann. Oft ist der Hersteller von mobilen Vorrichtungen gesetzlich verpflichtet, zu dokumentieren, welche Software-Module sich an Bord der von ihm hergestellten mobilen Vorrichtungen befinden. Beispielsweise aus diesen beiden Gründen wird nach der Übertragung mindestens eines der Software-Module die Information an die Zentrale übermittelt, ob das Software-Modul tatsächlich fehlerfrei an die mobile Vorrichtung übermittelt wurde (Anspruch 10). Bevorzugt wird nach jeder Übertragung eines Software-Moduls eine Information über das Ergebnis der Übertragung an die Zentrale übermittelt. Falls bei der Übertragung Fehler auftraten, wird bevorzugt zusätzlich eine Fehlerbeschreibung an die Zentrale übermittelt.

[0030] Durch die erfolgreiche Übertragung von Software-Modulen wird die aktuelle Konfiguration der mobilen Vorrichtung verändert. Insbesondere um gesetzlichen Auflagen nach einer Produktdokumentation nachzukommen, wird gemäß Anspruch 11 eine Rückdokumentation durchgeführt. Hierfür wird die Kennung der mobilen Vorrichtung zur Zentrale übermittelt. Diese Kennung unterscheidet diese mobile Vorrichtung wenigstens von allen anderen mobilen Vorrichtungen desselben Herstellers. In einem Konfigurations-Management-System wird die Information abgespeichert, welche Ziel-Geräte-Typen und welche Software-Module nach Abschluß der Übertragung an Bord der mobilen Vorrichtung tatsächlich vorhanden sind. Informationen über die Ziel-Geräte-Typen wurden erfindungsgemäß bereits für die Freigabe-Prüfungen an die Zentrale übermittelt.

[0031] Die Information, welche Software-Module fehlerfrei und unverfälscht übertragen wurden, wird auch für eine Synchronisation nach einem Fehlerfall, z. B. nach einem Verbindungsabbruch, verwendet. Ermittelt wird, welche Software-Module bei einem zweiten Versuch für die Übertragung vorgesehen werden.

[0032] Eine Übertragungs-Vorrichtung zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 11 umfaßt gemäß Anspruch 12 eine Einrichtung zur drahtlosen Datenübertragung zwischen Zentrale und mobiler Vorrichtung in beiden Richtungen und eine Steuerungs-Einrichtung, welche die Übermittlung von Software-Modulen von der Zentrale zur mobilen Vorrichtung veranlaßt und steuert. Die Steuerungs-Einrichtung ermittelt die aktuelle Konfiguration der mobilen Vorrichtung, wählt die Menge von Software-Modulen aus, und prüft, welche der ausgewählten Software-Module für die aktuelle Konfiguration freigegeben sind. Weiterhin veranlaßt die Steuerungs-Einrichtung die Übertragung der ausgewählten und freigegebenen Software-Module und ermittelt, welche Software-Module fehlerfrei an die mobile Vorrichtung übertragen wurden.

[0033] Bevorzugt reagiert die Steuerungs-Einrichtung auf erkannte Übertragungsfehler. Beispielsweise veranlaßt sie einen zweiten Übertragungs-Versuch, führt eine Fehlerbehandlung durch oder bricht die Übertragung der Software-Module ab.

[0034] Im folgenden wird ein Ausführungsbeispiel des erfindungsgemäßen Verfahrens anhand der beiliegenden Zeichnungen näher beschrieben. Dabei zeigen

[0035] **Fig.** 1 eine beispielhafte Ausführungsform der Erfindung, bei der die Software-Module von einer Zentrale mit Hilfe zweier verschiedener drahtloser Datenübertragungseinrichtungen zur mobilen Vorrichtung übertragen werden;

[0036] **Fig.** 2 eine beispielhafte Systemarchitektur für Zentrale und mobile Vorrichtung.

[0037] Im Beispiel der **Fig.** 1 wird wenigstens zeitweise eine Datenverbindung zwischen der Zentrale **10** und dem ersten Fahrzeug **20.1** und eine weitere Datenverbindung zwischen der Zentrale **10** und dem zweiten Fahrzeug **20.2** hergestellt. Die drahtlosen Datenverbindungen können auf die gleiche oder auf unterschiedliche Weisen hergestellt werden. Als zwei Beispiele sind in **Fig.** 1 die drahtlose Übertragung mit Hilfe eines Satelliten **50.1** und die über ein Mobilfunknetz **50.2** dargestellt. Die Software-Module werden z. B. über ein Weitverkehrsnetz oder ein lokales Netz übertragen. Die Zentrale kann sich an einem einzigen Ort befinden oder räumlich verteilt sein. Insbesondere falls ein Fahrzeug **20.1** oder **20.2** sich während der Übertragung bewegt, kann die übertragende Zentrale sogar während der Übertragung wechseln.

[0038] Bei der Übertragung von Software-Modulen werden für jedes der beiden Fahrzeuge **20.1** und **20.2** die folgenden Verfahrensschritte ausgeführt:

- Insbesondere dann, wenn der Fahrzeug-Hersteller die Software-Module nur dann übermittelt, wenn der Eigentümer der Übertragung der Software-Module zugestimmt hat und/oder die Software-Module bezahlt hat, wird eine Berechtigungsprüfung für die anfordernde Stelle durchgeführt. Hierfür wird beispielsweise ein Fingerabdruck einer anfordernden Person ermittelt oder eine PIN oder ein Paßwort von einer anfordernden Stelle erfaßt und anschließend Fingerabdruck, PIN oder Paßwort an die Zentrale übermittelt und bei einer Berechtigungsprüfung ausgewertet. Nach erfolgreicher Berechtigungsprüfung wird festgestellt, ob der Eigentümer der Übertragung verbindlich zugestimmt hat. Die folgenden Schritte werden nur dann durchgeführt, wenn eine Zustimmung vorliegt oder nicht erforderlich ist.
- Eine eindeutige Kennung des Fahrzeugs, vorzugsweise eine Fahrzeug-Ident-Nummer, wird ermittelt und an die Zentrale übermittelt. Diese Kennung unterscheidet das Fahrzeug von allen anderen Fahrzeugen dieses Herstellers. Zusätzlich werden die Baureihe, das Baumuster und das Baujahr und das Jahr der letzten Änderung übermittelt. Diese Informationen lassen sich zwar oft durch Lesezugriff auf ein zentrales Konfigurations-Management-System ermitteln. Werden sie aber vom Fahrzeug zur Zentrale übermittelt, so wird ein oft zeitraubender Lesezugriff eingespart.
- Die aktuelle Konfiguration des Fahrzeugs wird ermittelt und an die Zentrale übermittelt. Hierbei wird ermittelt, welche Ziel-Geräte vor Beginn der Übertragung an Bord des Fahrzeugs tatsächlich eingebaut sind und welche Software-Module vor Beginn der Übertragung an Bord des Fahrzeugs tatsächlich aktiviert und/oder abgespeichert sind. Vorzugsweise werden Typ-Kennungen für die aktuell eingebauten Geräte und bereits vorhandenen Software-Module, z. B. Sachnummern und Variantennummern, übermittelt. Diese Ermittlung wird bevorzugt dadurch ausgeführt, daß in jedem Ziel-Gerät ein Speicher vorhanden ist, in dem die Konfigurations-Informationen über dieses Ziel-Gerät abgespeichert sind und der z. B. über einen Datenbus angesprochen und ausgelesen wird. Alternative Ausführungsformen bestehen daraus, einen zentralen Speicher an Bord des Fahrzeugs oder Speicherchips, die an den Ziel-Geräten angebracht sind, auszulesen. Insbesondere dann, wenn ein Speicher in einem Ziel-Gerät aufgrund eines Defekts nicht ausgelesen werden kann oder wenn der Speicher eines neuen Ziel-Geräts noch nicht gefüllt ist, besteht ein Notbehelf darin, Markierungen an Geräten, z. B. Strichcodes, optisch zu erfassen.
- Bei Bedarf werden die Informationen über die aktuelle Konfiguration mit einem Datensatz über die Konfiguration des Fahrzeugs verglichen, der in einem Konfigurations-Management-System abgespeichert ist. Dies wird beispielsweise dann durchgeführt, wenn die übermittelten Informationen über die aktuelle Konfiguration lückenhaft oder erkennbar fehlerhaft sind. Zur Erkennung von derartigen Fehlern wird bevorzugt eine Plausibilitätsprüfung der vom Fahrzeug übermittelten und der abgespeicherten Informationen über die Konfiguration durchgeführt.
- Ausgewählt wird eine Menge von Software-Modulen, die von der Zentrale zum Fahrzeug übertragen werden.

Die Auswahl hängt von der aktuellen Konfiguration des Fahrzeugs, vom Anwendungsfall und von der Kundenanforderung ab.

– Nur diejenigen Software-Module werden übertragen, die für die aktuelle Konfiguration des Fahrzeugs freigegeben sind. Für jedes Software-Modul wird eine Freigabe-Prüfung durchgeführt, indem Freigabe-Informationen ausgewertet werden. Vorzugsweise bestehen diese Freigabe-Informationen aus Typ-Kennungen für Ziel-Geräte und Software-Module. Eine Ausführungsform wird weiter unten beschrieben. Mögliche Ergebnisse der Freigabe-Prüfung sind, daß alle, einige oder gar keines der ausgewählten Software-Module als freigegeben erkannt werden.

– Überprüft wird, ob die ausgewählten Software-Module jetzt übertragen werden können. Hierbei wird festgestellt, ob mit Hilfe der drahtlosen Datenübertragungseinrichtung überhaupt eine Verbindung zwischen Zentrale und Fahrzeug vorhanden ist oder aufgebaut werden kann und ob der Übertragungskanal eine für die Übertragung ausreichende Güte, insbesondere eine ausreichende Bandbreite besitzt. Diese Güte kann von dem sende- und Empfangsgerät **190** an Bord des Fahrzeugs abhängen. Beispielsweise wird eine untere Schranke für die Bandbreite oder eine obere Schranke für den Zeitraum, den die Übertragung in Anspruch nimmt, vorgegeben und mit der tatsächlich verfügbaren Bandbreite verglichen. Aus der tatsächlich verfügbaren Bandbreite und der Gesamtgröße der ausgewählten Software-Module wird bei Bedarf ein Wert für den Zeitbedarf der Übertragung vorhergesagt.

– Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden komprimiert, so daß die komprimierten Software-Module weniger Speicherplatz als die nicht komprimierten einnehmen. Bekannt sind verschiedene Verfahren zum Komprimieren von Daten.

– Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden für die Übertragung konvertiert. Bei Bedarf werden die Software-Module in Teile aufgeteilt. Gemeinsam mit jedem Software-Modul oder Software-Modul-Teil werden Meta-Informationen übertragen, die die Verteilung und Übertragung der Software-Module an Bord sowie deren Aktivierung steuern. Zu diesen Meta-Informationen zählen Parameter, die das verwendete On-Board-Übertragungsprotokoll benötigt.

– Die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module werden von der Zentrale zum Fahrzeug übertragen. Als Übertragungstechnik wird beispielsweise ein Mobilfunk-Standard, z. B. GSM oder UMTS, eingesetzt. Vorzugsweise wird ein zur gewählten Übertragungstechnik passendes Protokoll, z. B. das dateibasierte Protokoll zModem, verwendet. Dadurch wird insbesondere nach einem Abbruch der Verbindung eine sichere Fehlerbehandlung mit Synchronisation erleichtert, die weiter unten beschrieben wird.

– Vorzugsweise werden die übertragenen Software-Module an Bord des Fahrzeugs in einem Pufferspeicher abgespeichert

– Festgestellt wird, welche Software-Module fehlerfrei übertragen wurden. Diese Information wird an die Zentrale übermittelt. Beispielsweise wird nach jeder erfolgreichen Übertragung eines Software-Moduls eine Rückmeldung an die Zentrale übermittelt, oder nach erfolgreicher Übertragung aller Software-Module wird diese Information an die Zentrale übermittelt. Für die Feststellung wird vorzugsweise für jedes Software-Modul oder jedes Software-Modul-Teil eine Soll-Prüfsumme nach dem CRC-Verfahren ermittelt und übertragen. Nach der Übertragung wird an Bord der mobilen Vorrichtung eine Ist-Prüfsumme ermittelt und mit der Soll-Prüfsumme verglichen.

– Vorzugsweise werden Verschlüsselungs-Informationen gemeinsam mit den Software-Modulen übertragen, um zu prüfen, ob die Software-Module aus einer vertrauenswürdigen Quelle stammen und unverfälscht übertragen wurden. Beispielsweise wird ein Software-Modul in der Zentrale verschlüsselt und an Bord der mobilen Vorrichtung wieder entschlüsselt. Ein Verfahren hierfür ist aus DE 195 32 067 C1 bekannt. Oder ein Software-Modul wird unverschlüsselt, aber gemeinsam mit einer Signatur übertragen. Die Signatur wird mit Hilfe eines geheimen Schlüssels in der Zentrale erzeugt und mit einem öffentlichen Schlüssel verglichen, der beispielsweise zuvor auf einem anderen Kanal zur mobilen Vorrichtung übermittelt wurde.

– Falls festgestellt wurde, daß ein Software-Modul nur fehlerhaft, verfälscht oder gar nicht übertragen wurde, so wird ein zweiter Versuch der Übertragung durchgeführt. Falls zwischen erstem und zweiten Versuch eine größere Zeitspanne verstrichen ist, wird erneut die aktuelle Konfiguration des Fahrzeugs ermittelt, denn diese kann in der Zwischenzeit verändert worden sein. Scheitert auch der zweite Versuch, so wird die unten beschriebene Fehlerbehandlung durchgeführt.

– Daten über den aktuellen Betriebszustand des Fahrzeugs werden erfaßt und an die Zentrale übermittelt. Diese Daten umfassen beispielsweise die aktuelle Fahrgeschwindigkeit, den Motorzustand, den Ladezustand der Batterie und die aktuelle Position des Fahrzeugs. Aufgrund des Betriebszustands wird entschieden, ob die übertragenen Software-Module jetzt aktiviert werden. Dabei wird insbesondere geprüft, ob das Fahrzeug sich in einem sicheren Zustand befindet. Beispielsweise wird der Ladezustand der Batterie berücksichtigt, um sicherzustellen, daß während der gesamten Aktivierung genügend elektrische Spannung zur Verfügung steht. Die aktuelle Position wird beispielsweise ausgewertet, um zu prüfen, in welchem Land oder z. B. US-Bundesstaat sich das Fahrzeug befindet, um bei Bedarf zu prüfen, ob länderspezifische gesetzliche oder technische Randbedingungen zu beachten sind. Bei Bedarf wird der Fahrer des Fahrzeugs gebeten, das Fahrzeug in einen sicheren Zustand zu bringen, z. B. es anzuhalten, und dies zu bestätigen. Dies wird z. B. durch Sprachausgabe und -eingabe oder dadurch durchgeführt, daß Meldungen angezeigt werden und der Fahrer gebeten wird, diese zu bestätigen.

– Falls alle Software-Module fehlerfrei und unverfälscht übertragen wurden oder der Pufferspeicher vollständig gefüllt ist und falls das Fahrzeug sich in einem sicheren Zustand befindet, werden die übertragenen Software-Module aus dem Pufferspeicher in die Ziel-Geräte übertragen, vorzugsweise über einen Datenbus an Bord des Fahrzeugs. Bei Bedarf werden sie zuvor dekomprimiert. Für diesen Vorgang werden die Meta-Informationen ausgewählt. Nach der Übertragung zu den Geräten werden die Geräte bei Bedarf deaktiviert, die Software-Module aktiviert und danach die Geräte wieder aktiviert.

– In der Zentrale, z. B. in einem Konfigurations-Management-System, wird die aktuelle Konfiguration der mobilen Vorrichtung nach der Übertragung abgespeichert. Die aktuelle Konfiguration umfaßt die Informationen, welche der Ziel-Geräte an Bord tatsächlich eingebaut sind und welche Software-Module entweder fehlerfrei übertragen und ak-

tiviert wurden oder bereits vor der Übertragung aktiviert und durch die Übertragung nicht verändert wurden.
- Ein Konfigurations-Management-System in der Zentrale umfaßt einen Datensatz für das Fahrzeug. Dieser Datensatz wird nach der Übertragung aktualisiert, so daß er nach der Aktualisierung Informationen darüber enthält, welche der Ziel-Geräte an Bord tatsächlich eingebaut sind und welche Software-Module nunmehr aktiviert sind.
- Eine Fehlerbehandlung ist insbesondere dann erforderlich, wenn eine vorgegebene Anzahl von Versuchen Versuche scheitern, alle Software-Module fehlerfrei zu übertragen, beispielsweise weil keine Verbindung zwischen Zentrale und Fahrzeug hergestellt werden kann. Bevorzugt wird bei einer Fehlerbehandlung eine Synchronisation durchgeführt. Hierbei wird festgestellt, welche Software-Module fehlerfrei übertragen wurden. Der Datensatz für das Fahrzeug im zentralen Konfigurations-Management-System wird aktualisiert, und ein Fehlerprotokoll wird generiert. Zu einem späteren Zeitpunkt wird ein erneuter Übertragungsversuch begonnen, der von einem definierten Zustand ausgeht.

[0039] **Fig.** 2 zeigt eine beispielhafte Systemarchitektur für die Zentrale **10** und das Fahrzeug **20**. Die Zentrale **10** umfaßt die folgenden Komponenten:

- ein Central Remote Flashing Manager **160**, der die Übermittlung von Software-Modulen von der Zentrale zur mobilen Vorrichtung veranlaßt und steuert und dabei Software-Module auswählt und prüft, ob sie für die aktuelle Konfiguration freigegeben sind,
- ein Steuerungs- und Regelungs-Werkzeug **110**, mit dem die erforderlichen Maßnahmen zum Übertragen von Software-Modulen erfaßt und aufgelistet und veranlaßt werden und durch das die Durchführung der Maßnahmen überwacht wird,
- ein Logistiksystem **130**, das die benötigten Software-Module identifiziert, auswählt und für die Übertragung bereitstellt,
- ein Abrechnungs-System **140**, das die Übertragungsvorgänge kaufmännisch abwickelt und dabei insbesondere die Rechnungslegung durchführt und die Zahlungsvorgänge überwacht,
- ein Informationssystem **150**, das den Eigentümer und/oder Fahrer des Fahrzeugs vor der Übertragung über angebotene und durch Software-Module realisierbare funktionale Erweiterungen und Änderungen durch Software-Module und nach der Übertragung über die erfolgreiche Übertragung oder über aufgetretene Fehler informiert und das beispielsweise das Internet verwendet oder die Versendung von Briefen auslöst,
- ein Entscheidungsunterstützungs-System **170**, mit dessen Hilfe Software-Module in Abhängigkeit von der aktuellen Fahrzeug-Konfiguration und der durchzuführenden Kundendienst-Maßnahme ausgewählt werden,
- eine Sende- und Empfangseinrichtung **180** in der Zentrale und
- eine Sende- und Empfangseinrichtung **190**, die mit dem Fahrzeug verbunden ist.

[0040] Die Sende- und Empfangseinrichtungen **180** und **190** sind beispielsweise als Knoten eines Mobilfunknetzes, das z. B. mit den Übertragungsverfahren GSM oder UMTS arbeiten, oder für eine Übertragung mittels Satelliten ausgebildet. An Bord eines Fahrzeugs können mehrere Sende- und Empfangseinrichtungen **190** eingebaut sein.

[0041] Im folgenden wird an einem Ausführungsbeispiel beschrieben, wie die Freigabe-Prüfung durchgeführt wird und welche Freigabe-Informationen hierfür ausgewertet werden. In dem Ausführungsbeispiel werden zwei Ziel-Geräte an Bord eines Kraftfahrzeugs **20** mit Software-Modulen versorgt: eine Zentraleinheit eines Systems zur Sprachausgabe, die z. B. Meldungen an den Fahrer in natürlicher Sprache vorliest, und ein Steuergerät für das Türsystem. Die Zentraleinheit ist mit einem Sende- und Empfangsgerät für drahtlose Datenübertragung und über einen Datenbus mit dem Steuergerät verbunden.

[0042] Die beiden Ziel-Geräte stammen von unterschiedlichen Herstellern und werden in verschiedenen Varianten in Fahrzeuge eingebaut. Die Sprachausgabe soll in mehreren Sprachen möglich sein. Die Software-Module für alle Varianten der beiden Ziel-Geräte werden erzeugt und in der Zentrale abgespeichert.

[0043] Der Typ eines Ziel-Geräts und der eines Software-Moduls werden durch jeweils eine Sachnummer und eine Variantennummer gekennzeichnet. Die Sachnummer ist eine Abfolge von Ziffern und Buchstaben, die innerhalb des Produktspektrums des Fahrzeug-Herstellers eindeutig ist. Die Variante wird durch eine Zahl mit drei Ziffern gekennzeichnet.

[0044] Die Freigabe-Informationen sind beispielsweise in einer relationalen Datenbank in Form von Datensätzen in der Zentrale abgespeichert. Für eine Freigabe-Prüfung wird diese Datenbank eingelesen und ausgewertet. Ein Prinzip ist, daß ein Software-Modul nur dann für einen Typ von Ziel-Geräten freigegeben ist, wenn eine entsprechende Freigabe-Information in der Freigabe-Datenbank vermerkt ist, ansonsten nicht.

[0045] Jeder Freigabe-Datensatz umfaßt folgende Datenfelder:

- Baureihe
- Region
- Ziel-Geräte-Typen
- Zulieferer
- Beschreibung_Hardware
- Art_der_Software
- Software-Module
- Beschreibung_Software
- gültig_ab
- Voraussetzung

[0046] Mit "Baureihe" ist die Baureihe des Fahrzeugs gemeint, auf das sich der Freigabe-Datensatz bezieht, z. B.

W212. In den Datenfeldern "Ziel-Geräte-Typ" und "Software-Module" werden Geräte- bzw. Software-Typ-Kennungen aufgeführt, was im folgenden beispielhaft erläutert wird. Der in dem Datenfeld "gültig_ab" eingetragene Zeitpunkt legt für den Datensatz den Beginn des Freigabe-Zeitraums fest. Die im Datensatz genannten Software-Module sind nur dann für die genannten Ziel-Geräte-Typen freigegeben, wenn der Zeitpunkt der Übertragung nach dem durch das Datenfeld "gültig_ab" festgelegten Zeitpunkt liegt. Die Freigabe kann an eine Freigabe-Bedingung gebunden sein, die vorzugsweise als Boole'scher Ausdruck formuliert, wird. Die Inhalte der Datenfelder "Beschreibung Hardware" und "Beschreibung_Software" werden nicht automatisch ausgewertet. Sie erläutern vielmehr einem menschlichen Bearbeiter die Typ-Kennungen.

[0047] In dem folgenden Beispiel stammt die Software für die Zentraleinheit vom Zulieferer XY, die für das Tür-Steuergerät von den Zulieferern AB (für den europäischen Markt) und FG (für den US-amerikanischen Markt). Typen von Ziel-Geräten und Software-Module werden durch Sachnummern gekennzeichnet, die mit HW bzw. SW beginnen, gefolgt von drei oder vier Ziffern. Varianten sind durch drei Ziffern gekennzeichnet. SW-212-001 bezeichnet z. B. ein Software-Modul mit der Sachnummer SW-212 und der Variantennummer 001. Typ-Kennungen, zusammengesetzt aus Sachnummern und Variantennummern, sind in eckige Klammern gesetzt.

1. Datensatz

Datenfeld	*Inhalt*
Baureihe	W212
Region	EUR
Ziel-Geräte-Typen	[HW-1001-001] [HW-1001-002]
Zulieferer	XY
Beschreibung Hardware	Zentraleinheit für Europa
Art der Software	OS
Software-Module	[SW-101-001]
Beschreibung Software	Betriebssystem für Zentraleinheit, V1
gültig ab	1.1.1999
Freigabe-Bedingung	

[0048] Das Software-Modul [SW-101-001] ist durch den 1. Datensatz für die Ziel-Geräte-Typen [HW-1001-001] und [HW-1001-002] in Europa freigegeben.

2. Datensatz

Datenfeld	*Inhalt*
Baureihe	W212
Region	EUR
Ziel-Geräte-Typen	[HW-1001-001] [HW-1001-002]
Zulieferer	XY
Beschreibung_Hardware	Zentraleinheit für Europa
Art_der_Software	APPL
Software-Module	[SW-111-001]
Beschreibung_Software	Anwendung für Zentraleinheit, V1
gültig_ab	1.3.1999
Freigabe-Bedingung	

[0049] Das Software-Modul [SW-111-001] ist durch den 2. Datensatz für die Ziel-Geräte-Typen [HW-1001-001] und [HW-1001-002] in Europa freigegeben.

3. Datensatz

Datenfeld	*Inhalt*
Baureihe	W212
Region	USA
Ziel-Geräte-Typen	[HW-1002-001] [HW-1002-002]
Zulieferer	XY
Beschreibung_Hardware	Zentraleinheit für USA
Art_der_Software	OS
Software-Module	[SW-102-001]
Beschreibung_Software	Betriebssystem für Zentraleinheit, V1
gültig_ab	1.4.1999
Freigabe-Bedingung	

[0050] Das Software-Modul [SW-102-001] ist durch den 3. Datensatz für die Ziel-Geräte-Typen [HW-1002-001] und [HW-1002-002] in den USA freigegeben.

4. Datensatz

Datenfeld	*Inhalt*
Baureihe	W212
Region	USA
Ziel-Geräte-Typen	[HW-1002-001] [HW-1002-002]
Zulieferer	XY
Beschreibung Hardware	Zentraleinheit für USA
Art der Software	APPL

Software-Module	[SW-112-001]
Beschreibung Software	Anwendung für Zentraleinheit, V1
gültig ab	1.4.1999
Freigabe-Bedingung	[HW-1102-00n] AND ([HW-2102-001] OR [HW-2102-002]) AND NOT [HW-2302-00n]

[0051] Das Software-Modul [SW-112-001] ist durch den 4. Datensatz für die Ziel-Geräte-Typen [HW-1002-001] und [HW-1002-002] in den USA freigegeben, falls die Freigabe-Bedingung erfüllt ist. Die Freigabe-Bedingung ist erfüllt, wenn

- ein Ziel-Gerät vom Typ HW-1102 und einer der Varianten 001 bis 009
- und ein Ziel-Gerät vom Typ HW-2102 und der Variante 001 oder 002
- und kein Ziel-Gerät vom Typ HW-2302, das von einer der Varianten 001 bis 009 ist,

eingebaut ist. Hierbei ist 00n eine abkürzende Bezeichnung für die Varianten 001 bis 009.

5. Datensatz

Datenfeld	*Inhalt*
Baureihe	W212
Region	EUR
Ziel-Geräte-Typen	[HW-2001-001] [HW-2001-002]
Zulieferer	AB
Beschreibung Hardware	Tür-Steuergerät für Europa
Art der Software	TOOL
Software-Module	[SW-221-001]
Beschreibung Software	Diagnose für Tür-Steuergerät, V1
gültig ab	1.5.1999
Freigabe-Bedingung	[HW-2002-001] OR [HW-2302-00n]

[0052] Das Software-Modul [SW-221-001] ist durch den 5. Datensatz für die Ziel-Geräte-Typen [HW-2001-001] und [HW-2001-002] in Europa freigegeben, falls die Freigabe-Bedingung erfüllt ist. Die Freigabe-Bedingung ist erfüllt, wenn an Bord

- ein Ziel-Gerät vom Typ [HW-2002-001]
- oder ein Ziel-Gerät vom Typ HW-2302, das von einer der Varianten 001 bis 009 ist,

eingebaut ist.

6. Datensatz

Datenfeld	*Inhalt*
Baureihe	W212
Region	USA
Ziel-Geräte-Typen	[HW-2002-001] [HW-2002-002]
Zulieferer	FG
Beschreibung Hardware	Tür-Steuergerät für USA
Art der Software	TOOL
Software-Module	[SW-222-001]
Beschreibung Software	Diagnose für Tür-Steuergerät, V1
gültig ab	1.6.1999
Freigabe-Bedingung	[SW-221-001]

[0053] Das Software-Modul [SW-111-001] ist durch den 6. Datensatz für die Ziel-Geräte-Typen [HW-1001-001] und [HW-1001-002] in den USA freigegeben, falls an Bord das Software-Modul [SW-221-001] aktiviert ist.

[0054] Bei der Auswertung der Freigabe-Datei wird für jedes Ziel-Gerät, das im Fahrzeug vorkommt, die Freigabe-Datenbank durchsucht. Für jeden Datensatz wird das Datenfeld "Baureihe"' abgeglichen und das Datenfeld "Ziel-Geräte-Typen" ausgewertet. Ist an Bord ein Ziel-Gerät eines er im Datenfeld "Ziel-Geräte-Typen" genannten Typen eingebaut, so wird festgestellt, ob eine Freigabe-Bedingung formuliert ist. Ist dies der Fall, so wird geprüft, ob die Freigabe-Bedingung auf Erfülltsein geprüft. Ist die Freigabe-Bedingung erfüllt oder ist keine Freigabe-Bedingung formuliert, so sind alle Software-Module für das Fahrzeug freigegeben, die im Datenfeld "Software-Module" des Datensatzes genannt sind. Welche der freigegebenen Software-Module tatsächlich übertragen werden, hängt davon ab, welche Software-Module ausgewählt worden sind.

[0055] Für jedes Software-Modul werden weiterhin Konfigurations- und Sicherheits-Informationen beispielsweise in zwei Datenbanken für Software-Module und zwei für Software-Modul-Teile erzeugt, in der Zentrale abgespeichert und bei der Übertragung ausgewertet. Die eine Datenbank ist die Konfigurations-Datenbank, die andere die Sicherheits-Datenbank.

[0056] Die Informationen in der Konfigurations-Datenbank legen fest, welche Dateien zum Software-Modul gehören, wo diese Dateien abgespeichert sind und in welcher Reihenfolge sie wohin, d. h. zu welchem Ziel-Gerät, übertragen werden. Mit Hilfe der Sicherheits-Informationen werden Übertragungsfehler und Manipulationen erkannt.

[0057] Ein Datensatz für ein Software-Modul in der Konfigurations-Datenbank für Software-Module umfaßt beispielsweise folgende Datenfelder:

- Software-Modul
- Ziel-Adresse
- Größe
- Speicherort
- Prüfverfahren
- Prüfsumme
- Teile_Kennungen

[0058] Das Datenfeld "Ziel-Adresse" gibt die Ziel-Adresse des Ziel-Geräts auf dem Datenbus im Fahrzeug an, z. B. #57 für das Tür-Steuergerät und #20 für die Zentraleinheit.

[0059] Das Datenfeld "Größe" gibt die Größe des Software-Moduls in KByte an. Diese Angabe wird z. B. für eine Fortschrittsanzeige beim Übertragen verwendet. Festgestellt wird, wie viele KByte bereits übertragen sind, und durch die Angabe in der Konfigurations-Datei ist bekannt, wie viele KByte insgesamt zu übertragen sind. Der Quotient gibt den Arbeitsfortschritt an, der z. B. als Balken angezeigt wird.

[0060] Das Datenfeld "Speicherort" gibt an, wo dieses Software-Modul in der Zentrale abgespeichert ist, beispielsweise in Form eines Pfades eines Betriebssystems oder einer Zugriffsinformation auf eine Datenbank.

[0061] Das Datenfeld "Teile_Kennungen" ist nur dann ausgefüllt, wenn das Software-Modul nicht auf einmal, sondern in mehreren Teilen übertragen wird.

[0062] Beispielsweise umfaßt der Datensatz für das Software-Modul [SW-111-001] in der Konfigurations-Datenbank folgende Einträge:

7. Datensatz

Datenfeld	*Inhalt*
Software-Modul	[SW-111-001]
Ziel-Adresse	#20
Größe	256
Speicherort	/XY/EUR/APPL/V1
Prüfverfahren	CRC
Prüfsumme	4758A08C
Teile Kennungen	

[0063] Durch den 7. Datensatz wird festgelegt, daß die Übertragung des Software-Moduls [SW-111-001] mit dem CRC-Verfahren geprüft wird. Durch die Prüfung wird festgestellt, ob bei der Übermittlung zum Fahrzeug und der Speicherung an Bord des Fahrzeugs ein Übertragungsfehler aufgetreten ist. Als Prüfsumme wird ein CRC-Wert, in diesem Beispiel die Hexadezimalzahl 4758A08C, angegeben. Das Software-Modul wird auf einmal übertragen, daher ist das Datenfeld "Teile_Kennungen" leer.

[0064] Falls ein Software-Modul in mehreren Teilen übertragen wird, so werden jedem Software-Modul-Teil ein eigenes Prüfverfahren und eine eigene Prüfsumme zugewiesen.

[0065] Für jedes der Software-Modul-Teile wird in der Konfigurations-Datenbank für Teile ein eigener Datensatz mit

folgenden Feldern angelegt:

- Teile-Kennung
- Größe
- Speicherort
- Prüfverfahren
- Prüfsumme

[0066] Das Datenfeld "Speicherort" gibt an, wo dieser Software-Modul-Teil in der Zentrale abgespeichert ist.

[0067] Ein Datensatz in der Sicherheits-Datenbank umfaßt folgende Datenfelder:

- Software-Modul
- Ziel-Geräte-Typ
- Signatur

8. Datensatz

Datenfeld	*Inhalt*
Software-Modul	[SW-111-001]
Ziel-Geräte-Typ	[HW-1001-001]
Signatur	85A47D238

9. Datensatz

Datenfeld	*Inhalt*
Software-Modul	[SW-111-001]

Ziel-Geräte-Typ	[HW-1001-002]
Signatur	9CA47D236

[0068] Das Software-Modul [SW-111-001] ist in diesem Beispiel für zwei Varianten von Ziel-Geräten freigegeben, nämlich für die Varianten 001 und 002 des Typs HW-1001. Daher werden zwei verschiedene Signaturen erzeugt und in dem 8. und 9. Datensatz abgespeichert, nämlich eine Signatur pro Variante des Ziel-Geräte-Typs. Die Signatur für eine Variante wird vorzugsweise dadurch erzeugt, daß die Variante als Datenstrom behandelt wird und ein Hash-Wert erzeugt wird. Mit Hilfe eines geheimen Schlüssels wird aus diesem Hash-Wert die Signatur erzeugt. Die Signatur hängt also vom Software-Modul und vom geheimen Schlüssel ab. Für die Erzeugung der Signatur wird beispielsweise eine 1024-Bit-Verschlüsselung nach dem Algorithmus von Rivest-Shamir-Adleman (RSA-Verschlüsselung) verwendet.

[0069] Die Erzeugung von Signaturen wird auf einem Rechner durchgeführt, der streng gegen unberechtigten Zugriff und gegen Manipulationen geschützt wird. Beispielsweise betreibt der Zulieferer diesen Rechner und liefert die beiden Varianten und die beiden Signaturen an den Hersteller des Kraftfahrzeuges. Eine andere Ausführungsform ist die, daß der Zulieferer lediglich die beiden Varianten an den Hersteller liefert und dieser selber die Signaturen erzeugt. Beispielsweise übermittelt der Hersteller die Signaturen an den Zulieferer, und dieser überträgt die Software-Module auf seine Ziel-Geräte und verwendet dabei die Signatur für eine Prüfung. Eine dritte Ausführungsform besteht daraus, daß ein zertifiziertes Trust Center die Signaturen erzeugt und die geheimen Schlüssel verwaltet.

[0070] In einem permanenten, nicht überschreibbaren Speicher des Ziel-Geräts wird ein öffentlicher Schlüssel abgespeichert. Der öffentliche Schlüssel kann ausgelesen werden, er ist aber sowohl vor versehentlichem als auch vorsätzlichem Überschreiben oder Verfälschen oder Löschen geschützt. Vorzugsweise versieht der Zulieferer das Ziel-Gerät mit dem öffentlichen Schlüssel. Die Signatur wird nach dem Übertragen und vor dem Aktivieren des Software-Moduls mit Hilfe des öffentlichen Schlüssels geprüft. Durch diese Prüfung wird sichergestellt, daß das Software-Modul von einer vertrauenswürdigen Quelle kommt und nicht verfälscht oder manipuliert wurde.

[0071] Als On-Board-Übertragungsprotokoll wird beispielsweise das "Keyword Protocol 2000" (KWP2000) verwendet, das durch ISO 14230-1 und ISO 15765-1 bis 15765-4 und VDA 14230-1 bis VDA 14230-3 standardisiert wird. Befehle werden in KWP2000 durch Hexadezimal-Zahlen codiert, z. B. der Befehl "ReadEDUIdentification" (Auslesen einer Typ-Kennung für ein Ziel-Gerät) durch $1A,86. Die mit einem Software-Modul übertragenen Meta-Informationen umfassen die für das Protokoll KWP2000 notwendigen Kommunikations-Parameter, die die Übertragung an Bord vom

Pufferspeicher an ein Ziel-Gerät steuern, z. B. Blockgrößen, Timing-Parameter, Ablaufinformationen und Adresse des Geräts auf dem Datenbus. Andere Übertragungsprotokolle sind ebenfalls geeignet. Die Meta-Informationen werden beispielsweise ebenfalls in Form einer Tabelle übertragen. Diese Tabelle wird im Gegensatz zu der Tabelle für die Freigabe-Prüfung erst während des Übertragungsvorganges generiert.

[0072] Nachdem festgestellt wird, daß die ausgewählten und als freigegeben erkannten Software-Module fehlerfrei und unverfälscht übertragen wurden, werden mindestens folgende Informationen an die Zentrale übermittelt:

- eine eindeutige Kennung des Fahrzeugs,
- welche Software-Module fehlerfrei und unverfälscht übertragen wurden,
- welches Gerät, z. B. welcher Diagnosetester, für die Übertragung verwendet wurde
- und das Datum und der Zeitpunkt, zu dem die Übertragung abgeschlossen wurde.

[0073] Diese Informationen werden in der Zentrale, beispielsweise in einem Konfigurations-Management-System, abgespeichert, und zwar bevorzugt in dem Datensatz für das Fahrzeug. Dort wird weiterhin abgespeichert, wer die Übermittlung veranlaßt hat.

Patentansprüche

1. Verfahren zum Übertragen von Software-Modulen von einer Zentrale zu einer mobilen Vorrichtung, insbesondere zu einem Verkehrs- oder Transportmittel,
mit Hilfe einer Einrichtung zur drahtlosen Datenübertragung in beiden Richtungen,
wobei eine Menge von Software-Modulen ausgewählt wird,
dadurch gekennzeichnet,
daß
   - Informationen über die aktuelle Konfiguration der mobilen Vorrichtung an die Zentrale übermittelt werden, wobei diese Informationen eine Auflistung umfassen, welche Ziel-Geräte und welche Software-Module vor Beginn der Übertragung an Bord der mobilen Vorrichtung tatsächlich vorhanden sind,
   - geprüft wird, welche der ausgewählten Software-Module für die aktuelle Konfiguration freigegeben sind,
   - und die ausgewählten und für die aktuelle Konfiguration freigegebenen Software-Module übertragen werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß
   - für die Ziel-Geräte Geräte-Typ-Kennungen festgelegt werden,
   - für die Software-Module Software-Typ-Kennungen festgelegt werden,
   - unter Verwendung der Geräte-Typ-Kennungen und Software-Typ-Kennungen festgelegt wird, welche der ausgewählten Software-Module für welche Typen von Ziel-Geräten freigegeben sind
   - und diese Freigabe-Festlegungen bei der Freigabe-Prüfung verwendet werden.

3. Verfahren nach Anspruch 1 oder Anspruch 2, dadurch gekennzeichnet, daß
   - Informationen über eine der Zentrale bekannten Konfiguration der mobilen Vorrichtung in einem Konfigurations-Management-System oder Dokumentations-System abgespeichert werden
   - eine Kennung der mobilen Vorrichtung zur Zentrale übermittelt wird,
   - die an die Zentrale übermittelten Informationen über die aktuelle Konfiguration mit denen über die abgespeicherten Konfiguration verglichen werden
   und mindestens eine nicht übermittelte Information über die aktuelle Konfiguration durch Lesezugriff auf die abgespeicherte Konfiguration ergänzt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß vor der Übertragung der Software-Module geprüft wird, ob mit Hilfe der drahtlosen Datenübertragungseinrichtung ein Übertragungskanal mit einer für die Übertragung ausreichenden Güte aufgebaut werden kann.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß
   - Informationen über die Identität der Stelle, die die Übertragung der Software-Module anfordert, an die Zentrale übermittelt werden
   - und eine Berechtigungsprüfung für die anfordernde Stelle durchgeführt wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet,
   - für mindestens ein Software-Modul mit Hilfe eines geheimen Schlüssels eine Signatur erzeugt wird,
   - an Bord der mobilen Vorrichtung für mindestens ein Ziel-Gerät ein öffentlicher Schlüssel abgespeichert wird
   - und die Signatur mit Hilfe des öffentlichen Schlüssels geprüft wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet,
daß bei der Auswahl der Menge von Software-Modulen die aktuelle Konfiguration der mobilen Vorrichtung mit einer Soll-Konfiguration verglichen wird
und die Software-Module in Abhängigkeit von der Abweichung zwischen aktueller und Soll-Konfiguration ausgewählt werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet,
daß gemeinsam mit den Software-Modulen Meta-Informationen übertragen werden,
die die Verteilung und/oder Übertragung und/oder Aktivierung der Software-Module an Bord der mobilen Vorrichtung steuern.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet,
daß zusätzlich Informationen über den aktuellen Betriebszustand der mobilen Vorrichtung an die Zentrale übermittelt werden

in Abhängigkeit von den Betriebszustands-Informationen entschieden wird, ob die mobile Vorrichtung sich in einem sicheren Zustand befindet
und dann, wenn sie sich in einem sicheren Zustand befindet, die übertragenen Software-Module aktiviert werden.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet,
daß nach der Übertragung mindestens eines der Software-Module die Information an die Zentrale übermittelt werden,
ob das Software-Modul tatsächlich fehlerfrei an die mobile Vorrichtung übermittelt wurde.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, daß
- eine Kennung der mobilen Vorrichtung zur Zentrale übermittelt wird
- und in einem Konfigurations-Management-System die Information abgespeichert wird,

welche Ziel-Geräte und welche Software-Module nach Abschluß der Übertragung an Bord der mobilen Vorrichtung tatsächlich vorhanden sind.

12. Übertragungs-Vorrichtung zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 11, die
- eine Einrichtung zur drahtlosen Datenübertragung zwischen Zentrale und mobiler Vorrichtung in beiden Richtungen
- und eine Steuerungs-Einrichtung, die die Übermittlung von Software-Modulen von der Zentrale zur mobilen Vorrichtung veranlaßt und steuert,

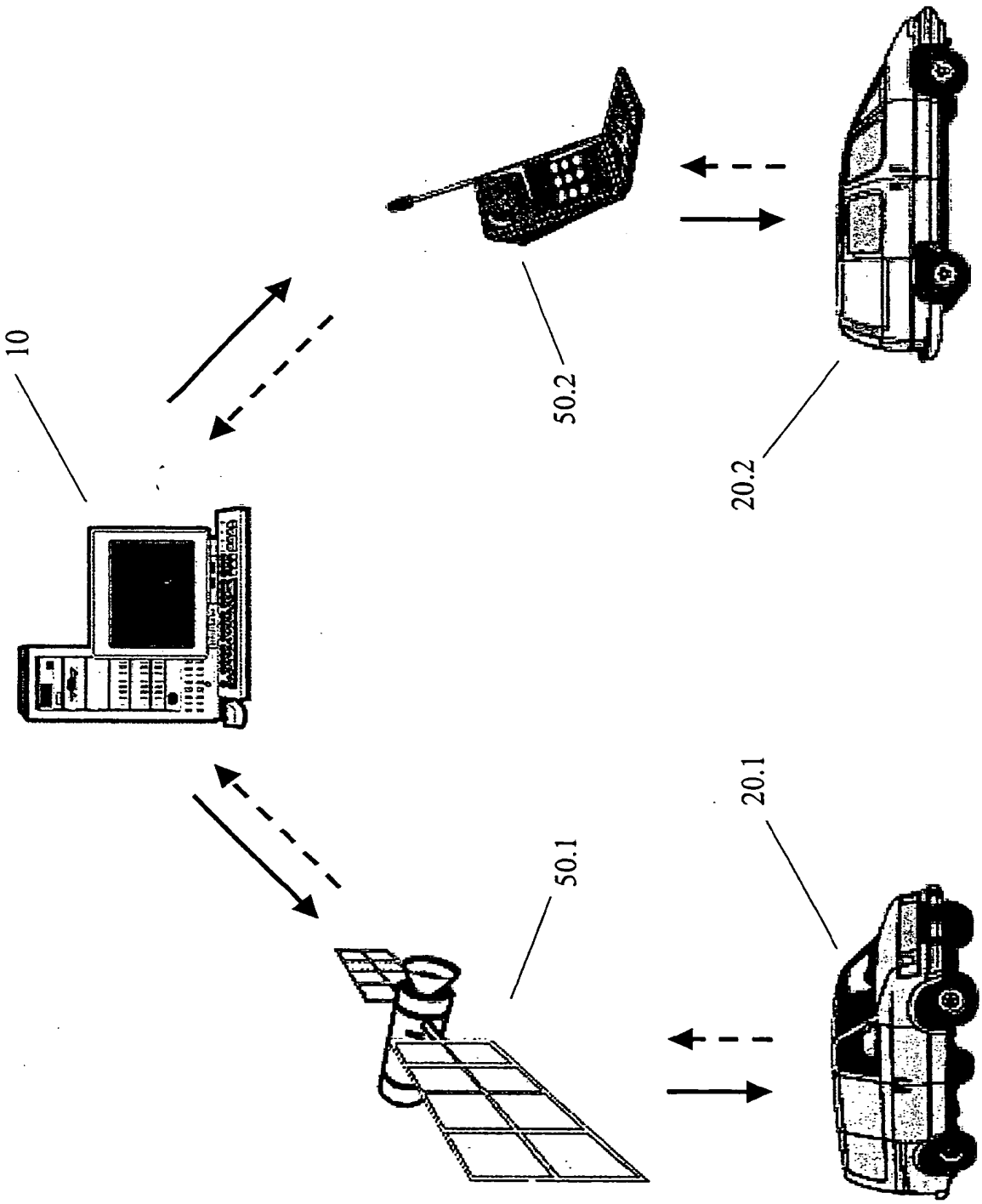
umfaßt,
dadurch gekennzeichnet,
daß die Steuerungs-Einrichtung
eine Einrichtung zur Ermittlung der aktuellen Konfiguration der mobilen Vorrichtung,
eine Einrichtung zur Auswahl der Menge von Software-Modulen
eine Einrichtung zur Prüfung, welche der ausgewählten Software-Module für die aktuelle Konfiguration freigegeben sind,
eine Einrichtung zur Veranlassung der Übertragung der ausgewählten und freigegebenen Software-Module
und eine Einrichtung zur Ermittlung, welche Software-Module fehlerfrei an die mobile Vorrichtung übertragen wurden,
umfaßt.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 31 395 A1
Int. Cl.[7]: G 08 C 17/02
Offenlegungstag: 23. Januar 2003

Fig. 1



Nummer: DE 101 31 395 A1
Int. Cl.[7]: G 08 C 17/02
Offenlegungstag: 23. Januar 2003

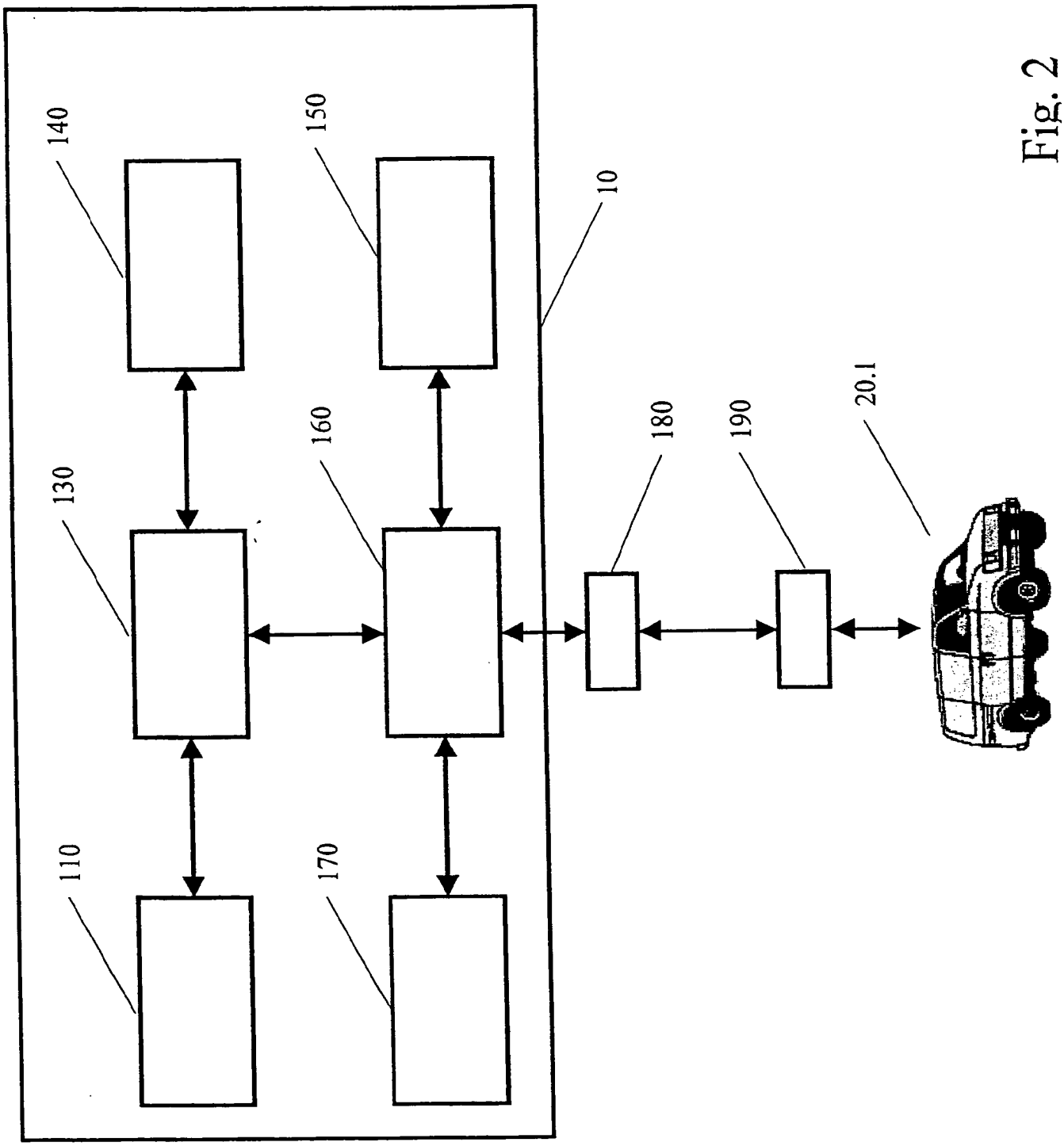


Fig. 2